LTR-NRC-12-6 NP-Enclosure

Response to NRC Request for Additional Information on the Software Program Manual for Common Q Systems (WCAP-16096-P, Rev. 2)

January 2012

Westinghouse Electric Company LLC
1000 Westinghouse Drive
Cranberry Township, PA 16066

1. SPM section 6.3.1 "Configuration Identification" specifies guidance for information to be included in header blocks for source files in order to maintain configuration identification. In the source files for the AC160, the header does not strictly follow this SPM guidance due to the process that creates those source files. Most of this information, including revision history, is instead contained in the footer of those files.

   Please provide revised SPM text used to address the issue described above.

   Westinghouse Response:
   Subsection 6.3.1 is being revised in Revision 3 of WCAP-16096-P to clarify that the source file information described is for "Westinghouse created Flat Panel Display Software and Custom PC Element Software." Also, the following is being added to describe the source file for AC160 Function Chart Type Circuits and Application programs:

   "AC160 Function Chart Type Circuits and Application Programs – Only the name and version/revision of the type circuit or application program is in the function chart diagram."

2. SPM Section 5.4.3.2.2, "Verifiers," under Validation and Verification (V&V) Team Roles states that "The verifier is also the independent reviewer for the design team." The audit team observed however that the V&V team did not perform this role.

   Please document in the response that the SPM will be revised to clarify that the V&V team verifier does not perform the role of independent reviewer for the design team.

   Westinghouse has also agreed to ensure that consistent terminology is used in the SPM and quality assurance implementing procedures. Please provide all changes to SPM terminology that will be made to address this generic action.

   Westinghouse Response:
   WCAP-16096-P, Rev. 2 incorrectly stated that the "Verifier is also the independent reviewer for the design team." Since that statement is not true, the following change will be made in subsection 5.4.3.2.2 of Revision 3:

   "IV&V reviews released documents that have been independently reviewed by the design team."

   In order to be consistent with internal procedures, the following terminology is being changed in WCAP-16096-P, Rev. 3:

   - The Preliminary Design Review (PDR) is being changed to the Architecture Design Review (ADR).
   - Revised Classification Assignment Record (RECAR) is being changed to Safety Classification Record.
   - The Verification and Validation (V&V) team is being changed to the Independent Verification and Validation (IV&V) team.
   - "Platform Lead" is being changed to "ELM" as the person responsible for the Common Q software during the Operation and Maintenance Phase.

3. SPM Section 4.6.2.9 states that:

"The Software Configuration Management Plan (SCMP) Review is held to evaluate the adequacy and completeness of the configuration management methods defined in the SCMP (SECTION 6) and their implementation. The review shall be performed by the V&V team, and results documented to identify all deficiencies found. The design team shall plan for the resolution of deficiencies."

Westinghouse stated that no review of the adequacy and completeness of Section 6, "SCMP," was performed by the WBN2 V&V Team since the NRC had approved the SPM (i.e., the NRC found the SCMP – SPM Section 6- to be adequate).

The NRC approved the SPM, in part, based on requirements it contained for future actions. The staff however understands this clause to mean that the V&V team will specifically evaluate the SCMP for acceptability and completeness for each development project. If the generic SCMP is determined to be unacceptable, then a project specific SCMP would need to be developed.

Please clarify how and when SCMP review activities will be performed in the next revision of the SPM. The staff also requests that a clarification of the objectives and scope of the SCMP review be included in this discussion.

Westinghouse Response:
WCAP-16096, Rev. 2 confused readers to believe that IV&V would review the adequacy and completeness of the Software Configuration Management Plan for each Common Q Project. However, the intent was to allow IV&V to review the generic SCMP (Section 6) once, and then reference their review for other Common Q projects. Therefore, the following is being added to subsection 4.6.2.9 of WCAP-16096, Rev. 3:

"By IV&V signoff of this SPM, the SCMP (Section 6) was reviewed and found acceptable by IV&V. Any comments resulting from their review have been incorporated. The IV&V team shall review and document the design team's adherence to the SCMP for each Common Q project."

4. SPM Section 6.2.2.1, "Requirements Phase" states:

"1. Define the software items that are to be controlled via this SCMP."

However, the V&V team for the WBN2 did not perform this activity during the requirements phase. Instead, the design team used the project plan to define the generic software that was used for WBN2 PAMS.

Please include a discussion in the revised SPM on generic vs. project-specific requirements. The SPM will also be updated to include a discussion to clarify in which part of the software life cycle these software items are to be defined.

Westinghouse Response:
Subsection 6.2.2.1 of WCAP-16096-P, Rev. 2, required a task to "define software items that are controlled via this SCMP." This led readers to believe that all software items that are controlled would be identified in the Requirements Phase. However, only ENM software is defined in the Requirements Phase, and the remaining software is not defined until the Implementation Phase. Therefore, the following changes are being made in the SCMP (Section 6) of WCAP-16096-P, Rev. 3:

- Subsection 6.2.2.1, Requirement Phase: "Define software items that are to be controlled via this SCMP" is being changed to "Define ENM software items that are to be controlled via this SCMP"

- Subsection 6.2.2.3, Implementation Phase: Task #1 is being added to say "Define software items that are to be controlled via this SCMP"

- Table II is being updated to reflect these changes.

5. SPM Section 4.5.2.1, "Coding Standards," states:

   "The V&V team shall review the applicable coding standards for each project for acceptability."

   Westinghouse credits the V&V signature on the generic coding standards document as addressing this requirement.

   Please clarify in the SPM to address project requirements for reviewing applicable codes and standards for acceptability.

   Westinghouse Response:
   In order to take credit for IV&V's review of the generic coding standards, the following statement is being added to subsection 4.5.2.1 of WCAP-16096-P, Rev. 3:

   "IV&V shall assure that the Common Q project uses an IV&V approved coding standards. If IV&V is a signatory on the generic Common Q coding standards, then this represents an evaluation of the acceptability of these standards for all Common Q projects."

6. Table 5.9-1 in Section 5.9 of the SPM provides software classification mapping to Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 1012-1998 which implies that the same or equivalent V&V tasks defined in IEEE 1012 are performed for the equivalent Westinghouse software classifications.

   Section 5.1 of the SPM also states this SVVP complies with IEEE 1012-1998. However, the V&V tasks defined in Section 5 of the SPM and in Exhibit 5-1 do not match the V&V tasks that are prescribed in IEEE 1012 Table 1, "V&V Tasks, Inputs and Outputs."

   In addition, Regulatory Guide 1.168 states that "software used in nuclear power plant safety systems should be [assigned software integrity level (SIL) 4] or equivalent as demonstrated by mapping between the applicants or licensee approach and SIL 4 as defined in IEEE Std. 1012-1998." The mapping provided in Table 5.9 and in Exhibit 5-1 does not demonstrate that an equivalent level of V&V is ensured for Software classified as "Protection."

Specifically, the Westinghouse SPM specifies a total of 23 tasks in Exhibit 5-1 while IEEE 1012 Table 1 specifies 62 V&V tasks that are required for SIL 4 software. Please provide documentation (mapping) to demonstrate that each of the V&V tasks specified in IEEE 1012 for SIL 4 software is being performed for Westinghouse "Protection" class software.

Westinghouse Response:
In order to show compliance to all of the IV&V activities defined in IEEE Std. 1012-1998, Westinghouse created a table that maps each activity in Table 2 of IEEE Std. 1012-1998 to the applicable section in WCAP-16096-P, Rev. 3 (Attachment A). Attachment A will be added as Exhibit 5-8 in Revision 3 of the SPM.

In some instances, the SVVP defined in Section 5 of WCAP-16096-P, Rev. 2, did not define all of the required IV&V tasks. Therefore, in order to conform to IEEE 1012-1998, the following are being added to WCAP-16096-P, Rev. 3:

- Subsection 4.3.2.2

  Deleted the following statement:
  "Test Plan Development continues into subsequent phases and is completed in the implementation Phase."

- Subsection 5.5.2.1

  Plant Documentation added as IV&V Input #6.
  User Documentation of ENM Software added as IV&V Input #7.

- Subsection 5.5.2.2

  Configuration Management Evaluation added as IV&V Task #6.
  Trace Project Baseline Documents added as IV&V Task #7.

- Subsection 5.5.3.2

  Development of a Common Q Specific Test plan added as IV&V Task #9.
  Configuration Management Evaluation added as IV&V Task #10.
  Hazard Analysis Review added as IV&V task #11.

- Subsection 5.5.3.3

  Test Plan added as IV&V Output #3.

- Subsection 5.5.4.2

  Criticality Analysis Review added as IV&V Task #5.
  Configuration Management Evaluation added as IV&V Task #8.
  Begin Test Procedure generation added as IV&V Task #9. IV&V Task #9 is being revised to:
  "Begin preparing module, unit, integration, and FAT test procedures in accordance with Reference 14, Section 7."
  Hazard Analysis Review added as IV&V task #10.

- Subsection 5.5.4.3

  Test Plan removed as IV&V output #4.

- Subsection 5.5.5.2

  Criticality Analysis Review added as IV&V #3.
  Begin Test Procedure generation removed as IV&V Task #10.
  Test Procedure generation added as IV&V Task #11.
  Hazard Analysis Review added as IV&V task #12.

- Subsection 5.5.5.3

  Test Procedure added as IV&V output #5.

- Subsection 5.5.6.2

  Test Procedure generation removed as IV&V Task #2.

- Subsection 5.5.6.3

  Test Procedures removed as IV&V output #1.

- Subsection 5.5.7.2

  Configuration Management Evaluation added as IV&V Task #7.

- Subsection 5.5.8

  The following is being added:

  "During this phase, IV&V shall evaluate the new system or software requirements to verify the applicability of this SVVP. Any necessary changes to the SVVP shall be documented in the Project Plan for the modification."

  The last two paragraphs are being revised to: "An IV&V report shall document all IV&V activities regarding the modification. This must include, or reference, a regression analysis including test requirements and results.

  A new code certificate must be prepared that references the original IV&V report, and the final IV&V report for the modification."

7. Many of the V&V tasks described in Section 5.2 of the SPM are not included in the table in Exhibit 5-1. Therefore, this table does not provide a complete mapping of all V&V activities required for the various classifications of software. In addition Section 5.5.2 of the SPM does not specify which organization is responsible for performance of these V&V activities. Please provide a complete listing of all V&V activities which includes the responsible organization for each activity. This list should either include all V&V activities specified for SIL 4 software in IEEE 1012 or provide mapping to those activities so that the staff can determine compliance with RG 1.168.

Westinghouse Response:
Exhibit 5-1 has "Requirements Verification" listed as a Software Requirements Phase task. The completion of this task encompasses the completion of all IV&V tasks defined in subsection 5.5.3.2 by the Independent V&V team. Likewise, "Design Verification" encompasses all of the tasks listed in subsection 5.5.4.2 and "Implementation Verification" encompasses all of the tasks listed in subsection 5.5.5.2 by the independent V&V team.

Attachment A also shows how the SPM fulfills all of the IV&V activities required by IEEE 1012-1998. The response to the previous RAI is relevant to this response.

8. There are no dedicated sections in the Westinghouse SPM for the following planning documents that are delineated in BTP 7-14 Section B.2.1.

a. Software Management Plan
b. Software Development Plan
c. Software Integration Plan
d. Software Installation Plan
e. Software Operations Plan

Each of these plans was previously evaluated on the basis of the required elements being contained within the existing sections of the Westinghouse SPM. However, with the exception of the Software Operation and Maintenance Plan (see RAI #9), no specific references were provided in the safety evaluation to SPM sections that can be credited to satisfy regulatory guidance or an acceptable, equivalent methodology or plans for the items listed above. The staff will need to evaluate the revised SPM against the acceptance criteria provided by the SRP for each of these planning areas. Please provide mapping to the applicable sections within the SPM or provide additional information to support the evaluation for each of these planning topics.

Westinghouse Response:
The criteria for a Software Management Plan and a Software Development Plan, as defined in BTP 7-14, are satisfied by a Project Plan and the Project Quality Plan (PQP). The Project Plan and the PQP are created on a project-specific basis. The glossary of Terms describes what is in a Project Plan. Revision 3 of the SPM augments the description with the following criteria to be in compliance with BTP 7-14:

- Overview of Project/System
- General functions of the software
- Assumptions/Dependencies/Constraints/Risks
- Methods, tools, and techniques
- Performance measures
- Security provisions
- Software Lifecycle

The Software Integration Plan is described in Section 7, Software Test Plan. Specifically, subsection 7.3.1.3 describes the details of the Integration Tests. Revision 3 of the SPM revises subsection 4.5.2.4 to add metrics for the integration tests. The Software Operations Plan is created on a project-specific basis, or will be the Licensee's responsibility.

The Software Installation Plan will be added in Revision 3 of the SPM. This plan will summarize the work instructions for installing software onto the hardware.

9. In the previous version of the SPM, Section 7 had been credited for combining the Operations and Maintenance aspects of the Common Q systems, however, in the new version; Section 8 is titled "Software Maintenance Plan." Was it Westinghouse's intent to limit the scope of this section to the Maintenance aspects of the software lifecycle or does this section still apply to both Operational and Maintenance aspects of the system lifecycle?

   Westinghouse Response:
   The intent of renaming the "Software Operations and Maintenance Plan" to the "Software Maintenance Plan" was to limit the scope to only Maintenance aspects of the system lifecycle. The Software Operations Plan is either a project specific activity, or the Licensee's responsibility.

10. Westinghouse referenced WCAP-16096 Section 11, "Secure Development and Operational Environment (SDOE) Plan," to address Interim Staff Guidance (ISG 6) Item 1.26 "Vulnerability Assessment." In reviewing Section 11 of WCAP-16096, the staff determined this planning document does not include all of the information needed to complete its assessment of the development aspects for the Common Q SDOE. The staff also performed a review of the Westinghouse Application Restrictions for Generic Common Q document and determined the required information is contained within the application restriction tables therein. The staff requests that the applicant submit the "Applications Restrictions for Generic Common Q" onto the docket to support the SDOE evaluation.

    Westinghouse Response:
    Westinghouse submitted documents, WNA-DS-01070-GEN-P and NP on the docket under transmittal letter, LTR-NRC-11-67.

11. Revision 3 of RG. 1.152 has already been issued; please clarify how Westinghouse intends to address this new version in the SPM.

    RG 1.152 Revision 1 (January 2006) is provided as Reference 17 in WCAP-16096, however, the staff will evaluate the common Q platform against the criteria of the current version of this standard. To support its review of the Common Q SDOE, the staff requests that Westinghouse provide an assessment of the Common Q system conformance to the criteria of RG 1.152 Revision 3. This assessment should address the criteria for each of the following software life cycle phases as specified in RG 1.152 Sections 2.1 through 2.5.

    a. concepts,
    b. requirements,
    c. design,
    d. implementation, and
    e. test.

    Westinghouse Response:
    Revision 3 of the Software Program Manual references RG 1.152, Rev. 3 (July 2011). See Attachment B for the SPM's conformance to the life cycle phase requirements of RG 1.152, Rev. 3.

12. In Table I., "Document Requirements," within the Documentation Requirements Section of the Common Q SPM several items specify that the listed document would be prepared by one of two or more individuals or teams. For example, the Test Plan (Item 25) is listed as being prepared by either the Design Team or the V&V Team. Please specify the conditions which would determine which of these individuals or teams would perform these activities.

Westinghouse Response:
The organization responsible for preparing software documentation depends on the safety classification of the software. Exhibit 5-1, Software Tasks and Responsibilities, defines which organization is responsible for performing specific software lifecycle tasks based on the classification of the software.

A note will be added to Table I in Revision 3 of the SPM. This note will point the reader to Exhibit 5-1 wherever the design team or IV&V team are listed as the responsible organization.

13. In Table II. "Information Requirements," several of the Output Documents are listed as "V&V Report" with no delineation of what type of V&V Report would need to be created to document this activity or identification of during what part of the development life cycle this report would be generated. Is there only one V&V Report which is updated as the development process progresses or are there multiple V&V reports created throughout the development process?

Westinghouse Response:
The term "V&V report" refers to the IV&V Phase Summary Report that is produced at the closure of each software lifecycle phase. This is defined in subsection 5.6.1, which states: "IV&V phase summary reports: These reports are issued after each life cycle phase of the IV&V task to summarize the IV&V review. Phase summary reports may be consolidated into a single report if desired."

14. It is unclear to the staff at which phase of the development process each output document listed in Table II would be created to document the associated activity. Please provide additional information to identify the phase within the software development process during which each listed output document would be created.

Westinghouse Response:
Attachment C shows in what phase each output document in Table II is created.

15. In Table II. "Information Requirements," what is meant by the requirement listed in SPM Section Number 10.2 describing the, "Justification for not performing complete system testing"? Section 10.2 describes error reporting and includes a discussion of determining the extent of retest but does not include any discussion of not performing complete system testing. If this document is only referring to the retest requirements as described in Section 10.2 then the document title should not imply that a test requirement is being omitted.

Westinghouse Response:
In certain instances, it might not be required to perform a complete system retest to test a change in the software. If this is the case, justification for not performing the complete system retest must be documented in the regression analysis of the Exception Report or on the Software Change Request (SCR). Therefore, Table II is being revised in Revision 3 to change "testing" to "retesting."

16. In Subsection 1.2.1 "Software Classification and Categorization," the use of the term "General Purpose software" is used. The examples cited reference test software such as that utilized for a commercial dedication process. Any such software would be subject to the restrictions of IEEE 7-4.3.2 Section 5.3.2 and would have to be qualified based upon the tool usage and the subsequent downstream testing performed on the safety related components being tested by the tool. Please include appropriate qualifiers for the examples listed so that the implication that all test software being used could be classified as general purpose software.

    Westinghouse Response:
    The description of General Purpose software in subsection 1.2.1 of Revision 3 will be modified to:

    "Examples of commercially dedicated General Purpose software include compilers, assemblers, linkers, comparators, and editors. Examples of Westinghouse developed General Purpose software include test case generators, and test tools (e.g., I/O Simulator)."

17. Within Section 3.3.1 "Organization and Responsibilities," the SPM discusses that the Quality organization has a matrix reporting relationship to the Senior VP of the NA business unit. The staff requires additional information in order to determine if an adequate level of independence has been established. Please provide a detailed listing of all reporting relationships established to demonstrate that an adequate level of separation exists between the Quality organization and the organizations with which it conducts its business function.

    Westinghouse Response:
    Revision 3 of the SPM, Exhibit 2-1, Design/IV&V Team Organization, is being updated to summarize the current Westinghouse organization. Accordingly, subsection 3.3.1 was updated to state:

    "The Quality organization has a reporting chain separate from the design team such that the QA organization is independent of project schedule and cost considerations."

    Section 2 will also be updated in Revision 3 to summarize the Westinghouse organization.

    Exhibit 2-1 is being provided in Attachment D.

18. Within Section 3.3.2 "Resources," of Section 3, Software Safety Plan, the SPM previously stated that, "Project schedules and resource allocations are established and maintained in SAP."

    It now states, "Project schedules and resource allocations are established via the Project Plan."

    However, in Table II "Information Requirements" of the Documentation Requirements Section it states that a detailed schedule and Resource Plan are documented in the Systems, Applications and Products in Data Processing (SAP), an enterprise software system utilized by Westinghouse.

    Please explain which information is correct?

    Westinghouse Response:
    Table II was updated to change the output document for these tasks from "SAP" to "Project Plan."

19. Section 3,"Software Safety Plan," Section 3.3.5.7.3 "Test Reports," it states:

The test reports document the execution of the acceptance test procedures. In addition to attaching the signed and checked off test procedure, the test reports provide an overall summary of the test results and the resulting Exception Reports generated during the test. The system configuration at the time of test execution is also documented in the test reports. Test Reports are prepared in accordance with Reference 14, Section 10.

In reviewing Section 10 of Reference 14 – IEEE Std. 829 – 2008, the section is the "Level Test Design" section which has nothing to do with Test Reports as is implied. On the other hand, Section 14 Anomaly Report, of IEEE Std. 829 – 2008 describes a similar process and may have been the intended reference.

For reference, in IEEE Std. 829 – 1998, Section 10 is the Test Incident Report.

Please explain the reason for referencing Section 10 of Reference 14 in relation to Test Reports or provide a corrected reference.

Westinghouse Response:
Revision 2 of the SPM was referencing the wrong year and corresponding sections to IEEE Std. 829. After an evaluation, it was determined that IEEE Std. 829-1998 should be referenced since it is endorsed by the latest revision to RG 1.170. The SPM was reviewed to make sure the appropriate sections of IEEE 829-1998 are referenced. Accordingly, Revision 3 changed Reference 14 section numbers from Sections 3, 6, and 10, to Sections 4, 7, and 11, respectively.

20. Section 4, "Software Quality Assurance Plan," Section 4.1.1 "Purpose," it previously stated, "NuCARs [now referred to as RECARs] shall be prepared by the design team and reviewed by the V&V team. The text has been modified to remove the requirement for the V&V team to conduct a review of the software classification determination. Please provide justification for removal of this requirement including a discussion of what organization now performs this validation and/or verification activity?

Westinghouse Response:
In Revision 3 of the SPM, Revised Classification Assignment Record (RECAR) is being changed to Safety Classification Record.

Revision 3 of the SPM changes the last sentence of subsection 4.1.1 to say:
"The Safety Classification Records are prepared by the design organization and are an input to the design and IV&V teams to determine the necessary requirements for design and IV&V activities. The appropriateness of the software safety classification is reviewed throughout the design and IV&V activities."

21. In Section 4.3.2.6 "Site Installation and Checkout Phase," the SPM discusses the use of an Exception Report Log. Additionally, the detailed record of changes states that "The Test Exception Report (TER) form is used to document all software anomalies, not just test exceptions."

Because of this characterization, it is not clear to the staff why is there no mention of this formal corrective action mechanism earlier in the development process in Sections 4.3.2.1 through 4.3.2.4. Please provide a definition of the TER which includes a discussion of when during the

development process they will be used to document software anomalies.

Westinghouse Response:
The term Test Exception Report (TER) was changed to Exception Report in Revision 2 of the SPM.

The SPM did not mention the use of Exception Reports (ERs) until the Test Phase of the development process. Since ERs are used as a formal corrective action mechanism earlier in the development process, the following statement is being added to Revision 3, subsections 4.3.2.1-4.3.2.5:

"The IV&V team reviews the design team's outputs during this phase. Any anomalies found will be documented using Exception Reports."

22. Section 4.4 "Documentation," Section 4.4.1 "Purpose," the text states, "If required, documents listed shall be made lifetime quality records in accordance with Reference 4" [Westinghouse Level II Policies & Procedures, Revision 15]. Where in the SPM or other appropriately cited Westinghouse document does the text describe the requirements for the need to create lifetime quality records?

Westinghouse Response:
The requirements for the need to create lifetime quality records are defined in Westinghouse Level II Procedure (Reference 4 of the SPM), WEC 17.1.

23. Section 4.4 "Documentation," Section 4.4.1 "Purpose," the text states, "If required, documents listed shall be made lifetime quality records in accordance with Reference 4" [Westinghouse Level II Policies & Procedures, Revision 15]. Please provide a description of the criteria that is used to determine the retention requirements for Common Q records.

Westinghouse Response:
The requirements for a lifetime quality record, as defined in Westinghouse Level II Procedure WEC 17.1, are the following:

[

]^{a,c}

24. Section 4.5 "Standards, Practices, Conventions and Metrics," Section 4.5.2.2 "Software Testing Standards," states:

"Specific format and content...shall comply with Reference 14, Sections 6 and 10."

However in the new revision of Reference 14 [IEEE Std. 829 – 2008], Section 10 is the Level Test Design" section, not the Test Incident Report section as was the case in the 1998 revision of the IEEE Std.

Westinghouse Response:
Revision 2 of the SPM was referencing the wrong year and corresponding sections to IEEE Std. 829. After an evaluation, it was determined that IEEE Std. 829-1998 should be referenced since it is endorsed by the latest revision to RG 1.170. The SPM was reviewed to make sure the appropriate sections of IEEE 829-1998 are referenced. Accordingly, Revision 3 changed Reference 14 section numbers from Sections 3, 6, and 10, to Sections 4, 7, and 11, respectively.

25. Section 4.5.3 "Life Cycle Application of Standards" informs the reader to refer to Section 5.5 "Life Cycle Verification and Validation," for the application of these standards, practices, conventions, and metrics at each life cycle phase. It is not clear to the staff what specific standards and/or conventions and/or metrics are being referred to in the text. Section 5.5 does not appear to include a discussion of any specific standards, practices, conventions or metrics either. Please provide an explanation of which standards, practices, conventions, and metrics are applicable to which phases of the software development life cycle.

Westinghouse Response:
Subsection 4.5.3 is being deleted. This information can be found in subsections 4.5.2.1, 4.5.2.2, and 4.5.2.3.

26. Within Section 5.4.3.2.3 "Librarian," the individual previously had responsibility for records retention and revision control of the software product(s) and ensures procedures concerning the management of software recordkeeping were enforced. It is not clear to the staff whether that responsibility has been removed or if the responsibilities described in the re-worded sentence are equivalent. Please explain the purpose of this revised wording and include a discussion of who (by position or title) has the responsibility for performing the following activities:

    a. Records retention
    b. Revision control of software products
    c. Enforcement of procedures for managing software record keeping

Westinghouse Response:
Subsection 5.4.3.2.3 was revised to provide a clearer definition of the Librarian's responsibility. The records retention of software modules in use and their revision levels is now the responsibility of the author of the software release record by archiving the record in the Westinghouse document management system. The task of assuring that "the procedures for software changes are followed" was removed as a Librarian responsibility because this task is the responsibility of the EPM.

Other References to "software librarian" will be reviewed and revised in Revision 3.

27. In Section 5.4.5.2 "V&V Core Activities," Item 6 discusses that either the design team or the V&V Team will provide the report qualifying such an item. Please explain the criteria used to determine which organization will perform this activity. This discussion should include a description of how the required levels of independence are maintained for all Common Q software.

Westinghouse Response:
Subsection 5.4.5.2, task #5 is being modified to say:
"A Commercial Grade Dedication report is prepared by the design team. The IV&V team shall review the report to determine its applicability and suitability for meeting the system requirements."

Likewise, the first paragraph of subsection 5.5.3.2, task #7 is being modified as follows:

"The Design team reviews previously developed or sub-vendor software in the following areas and produces a Commercial Grade Dedication Report stating whether this software is adequate for its intended use. The IV&V team reviews the Commercial Grade Dedication Report to evaluate the suitability of the commercially dedicated item for the particular implementation being verified."

28. In Section 5.4.5.3, Requirements Traceability Analysis, the second paragraph below the "Requirements, Design, Code and Test" diagram, the word analysis has been replaced with matrix. However, the next sentence within the paragraph goes back to describing the analysis. Please describe the relationship between the RTA and the RTM including a discussion of how one affects the other and which individuals and organizations will perform given functions for both the RTA and RTM.

Westinghouse Response:
The Requirements Traceability Matrix (RTM) is either a table of information prepared manually, or a report generated from a requirements database. The RTM associates requirements with the documentation and software that satisfies them. Requirements are entered in the matrix and are organized into successive lower level requirements as described in each document. The requirements are then traced through the software lifecycle to the design, code, and test documentation. The design team is responsible for creating the RTM to the point of identifying the code satisfying the requirement. IV&V will complete the RTM identifying validation of the requirement.

The Requirements Traceability Analysis (RTA) is the task of ensuring the completeness and accuracy of the RTM; all lower level requirements and design features are derived from higher level requirements, and that all higher level requirements are allocated to lower requirements, design features, and tests. The traceability analysis also provides a method to cross-reference each software requirement against all of the documents and other software items in which it is addressed. The purpose of this analysis is to ensure that the design team addresses every requirement throughout the design life cycle process. The IV&V team is responsible for performing the RTA.

These definitions will be added to the Glossary of Terms in Revision 3 of the SPM.

In Revision 3, Subsection 5.4.5.3 will be revised to organize the description of the RTM and RTA. The RTM will be described in the beginning of the section, and the RTA will be described in the end of the section.

29. The software Problem Report Exhibit 6-3 was deleted from Section 10 per detailed record of changes (see page ix). However, within Section 6.1.1 Purpose, of Section 6.1 Software Configuration Management Plan, Item 5 reads, "Maintain the status of released software, users of this software and associated **problem reports**." The term Problem Report is also used elsewhere

in the document (Item 5 of Section 6.2.2.6, Section 4.1.2, 8.2.4, and in Section 9.5.2). This RAI applies to Item 8 of Section 6.1.1 also.

It is not clear what the "problem reports" being referred to are, in light of the fact that the software problem report has been deleted from Section 10. It is the staffs understanding that "Exception Reports" are now used to identify internal software problems. Please explain what is meant by the term problem report throughout the document and what, if any similar document or documents replaced the problem report.

Westinghouse Response:
The staff is correct, the Exception Reports are now used to identify both internal and external software problems. Therefore, Revision 3 of the SPM changes "problem report" to "exception report" where applicable.

30. Section 6 "Software Configuration Management Plan," Section 6.3.4 "Configuration Audits and Reviews," Item 5 states the V&V team will conduct a functional review to verify "actual" functionality and performance is consistent with the System Requirements Specification. The staff understands that equipment functionality is not exercised during a functional review activity. Additionally, the stated purpose of a functional review in Section 4.6.2.5 differs from the purpose stated in Section 6.3.4. In Section 4.6.2.5 it states that a functional review is conducted to "verify that all requirements specified in the Software Requirements Specification have been met." Please explain how a functional review can satisfy the statement in Section 6.3.4.

Westinghouse Response:
The purpose of Items 4 through 6 in Section 6.3.4 of the SPM is to define the QA and IV&V roles and responsibilities for these SQAP activities. In order for Item 5 to be consistent with the SQAP, Item 5 is being revised as follows, "5. A functional review shall be performed in accordance with subsection 4.6.2.5 by the IV&V team prior to shipment to verify that all requirements specified in the Software Requirements Specification for the software configuration items have been met. This will be accomplished by the IV&V requirements traceability analysis."

31. Section 6, Software Configuration Management Plan, Section 6.3.6.1 "Subcontractor Software," of the last sentence states, "Proprietary item ownership security and traceability does not apply since Westinghouse owns the rights of subcontractor software." The term "Proprietary Item Ownership security and traceability" is not used elsewhere in the SPM so it is not clear to the staff what specific activities are not applicable for Subcontractor Software. Please explain, in greater detail, what is meant by that statement.

Westinghouse Response:
This sentence is addressing Section 3.3.6 e) in IEEE 828-2005, in which, for subcontracted software, the software configuration management plan must address, "How proprietary items will be handled for security of information and traceability of ownership (e.g., copyright and royalties)." Since Westinghouse owns the rights of subcontracted software, this aspect of the configuration management plan does not need to be addressed.

To clarify, subsection 6.3.6.1 will be updated in Revision 3 to state:

"Westinghouse does not need to plan for how proprietary items will be handled for security of information and the traceability of ownership because Westinghouse owns the rights of subcontracted software."

32. Section 7 "Software Test," Section 7.3.1.2 "Unit Testing, Plan," describes the steps taken by Westinghouse for Unit Testing. In Section 4.2.3.5 "Testing Phase" of Section 4, Software Quality Assurance Plan, the text states that Module and Unit Testing will be conducted in accordance with Reference 12, IEEE Std. 1008 – 1987, IEEE Standard for Software Unit Testing. IEEE Std. 1008 – 1987 specifies when conducting unit testing to test for input, output and internal states of software units. However, the following statement in Section 7.3 of the SPM implies that internal states are not tested during unit testing.

    SPM Section 7 "Software Test Plan," Section 7.3 "Testing Process Activities and Tasks," of states that testing for internal states will only be conducted for module tests. Please provide a description of how the Unit testing that is performed on Common Q software tests for internal states of the software to comply with IEEE Std. 1008 – 1987.

    Westinghouse Response:
    Since Westinghouse is testing internal states at the module level rather than at the unit level, subsection 4.3.2.4 is being revised to:

    "Module and unit testing shall be performed in accordance with Section 7 and Reference 12. Internal state testing is conducted during module testing."

    Also, subsection 5.5.8 will be updated in Revision 3 to add the following statement:

    "See Section 7 for the Common Q testing methodology."

33. Section 10 "Problem Reporting and Corrective Action," Section 10.2 "Error Reporting Before Software Approval for Use," the third paragraph that previously contained requirements that the Exception Reports be forwarded to the EPM, the ELM, and the V&V team have been removed.

    Please provide an explanation of why these actions were taken including a description of what equivalent mechanisms have been put in place to ensure errors are properly identified, captured, tracked, resolved and placed into a records management system to ensure the issue is available for historical reference.

    Westinghouse Response:
    Since an exception report is generated as a result of an error finding, it was not necessary to include project management (EPM and ELM) to the exception report signoff process due to the independence of the test team from the design team. If an SCR is generated as a result of an exception report then project management is included in the signoff process. IV&V reviews all exception reports for safety-related software outside the ER signoff process and documents this review in the phase summary report. The error reports are not placed in the Westinghouse records management system. However, the error reporting system is on a corporate network server that is backed up for disaster recovery.

34. In Section 1.4 and throughout the SPM, it is unclear to the staff whether the requirements invoked by the use of the word "shall" would apply to the platform hardware and software, or to the application specific hardware and software, or to both. Please explain whether the use of "Shall" or "Should" in the SPM is intended to document activities to be performed on each application.

    Westinghouse Response:
    In order to clarify the applicability of this SPM, the following is being added to Section 1.4:

"Any software developed under a different program than this SPM will go through a Commercial Grade Dedication process, which evaluates the development of that software to the requirements of the SPM. A Commercial Grade Dedication Report will be produced for this software."

35. The staff would like to know if this version of the SPM is intended to supersede all previous versions that have been referenced in Common Q applications. Because this revision describes several substantial process changes, it is unclear to the staff what actual processes were used for development of specific applications that refer to previous versions of the SPM. For applications that are currently under review, the staff would like to have a clear understanding of the processes that are being used for system development.

    Please describe how the revised processes defined in Revision 3 of the SPM have been applied to those applications under review that currently reference previous versions of the SPM.

    Westinghouse Response:
    The SPM was revised to this version to be consistent with Westinghouse's internal policies and procedures. Currently for every project, Westinghouse must document the differences in process described in the currently approved SPM and the process used today. Therefore, this revised SPM will be referenced for future applications.

36. The Common Q Platform Topical Report WCAP-16097 discusses the use of Custom PC Elements in Section 5.2.1.2.3 which states that these elements will be subject to the requirements set forth in the SPM. However, Custom PC elements are not mentioned in the SPM.

    Please provide additional information on how the SPM controls are applied to the development of Custom PC elements.

    Westinghouse Response:
    The definition for "module" in the SPM refers to "custom PC Element," as defined in the Glossary of Terms. Therefore, any requirements on a software module apply to custom PC elements.

37. Section 4.6.2.3 "Code Verification," discusses the use of Code Reviews as a means of ensuring that source code conforms to software coding standards and guidelines. The staff requires additional information on how these code reviews are performed in order to determine if this SQA activity adequately satisfies the criteria of BTP 7-14 Sections B.3.3.4 and B.3.1.3.4. Please provide a detailed description of the Code Review process. This description should include a discussion of how the code which is developed for Custom PC elements is reviewed in a manner to ensure that high quality software which is capable of performing all required safety functions is produced.

    Westinghouse Response:
    Review of the AC160 Function Chart, FPD application C source code or AC160 custom PC element source code focuses on verifying that the implementation meets the appropriate criteria presented in the applicable code review checklists (See Attachments E1 – E3). Completion of the checklist provides evidence of the code review and verification. Each checklist is attached to the Code Review Report.

38. Please confirm if the checklists in Exhibits 5-2, through 5-6 will be included in the V&V summary reports. If not, then how will completion of these checklists be documented? Please

provide a description of how these checklists will be used including a description of all documentation requirements associated with performance of these activities.

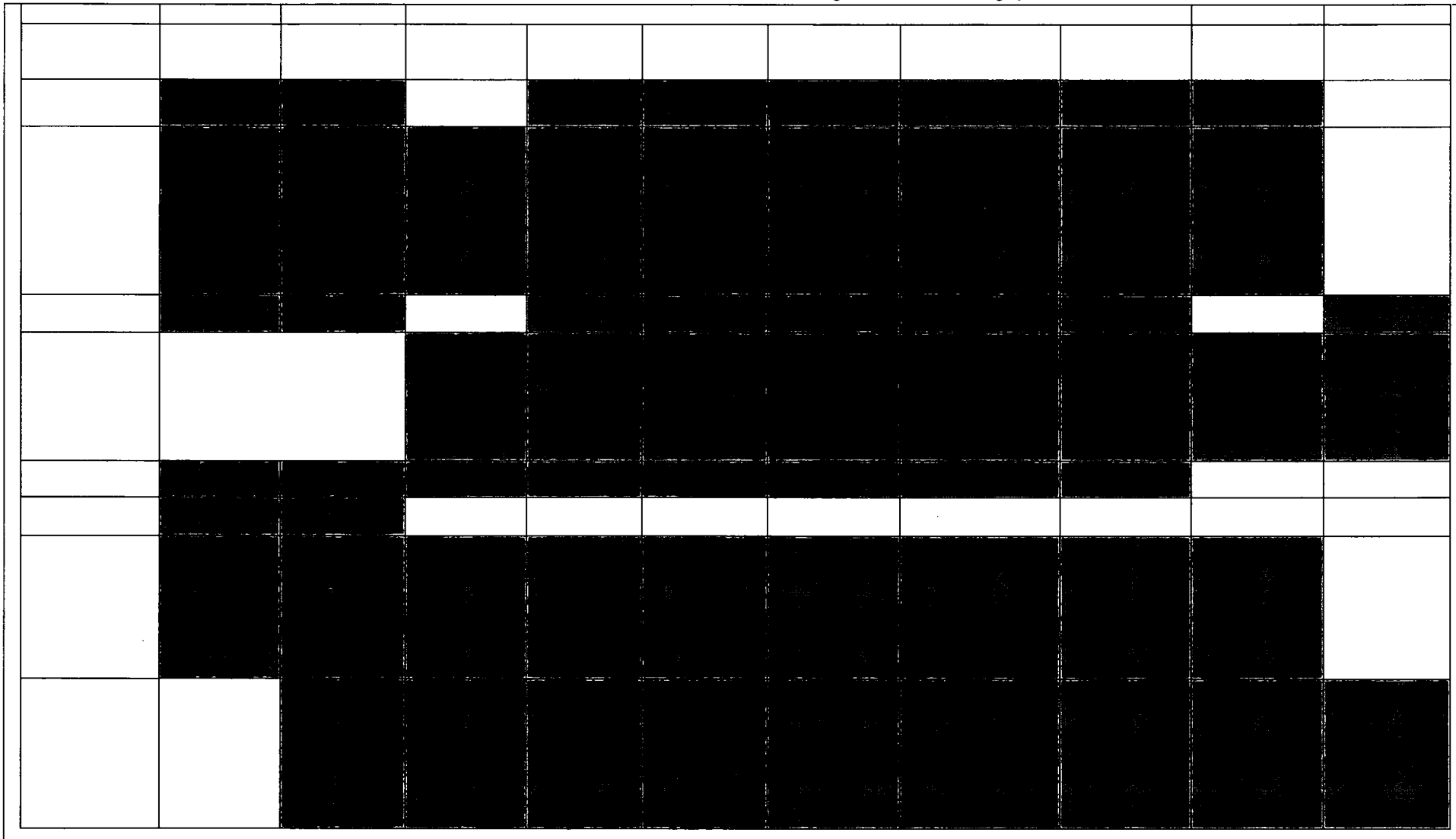
Westinghouse Response:
Exhibits 5-2 through 5-7 will be included in the IV&V Phase Summary Reports. To ensure they are included, a new checklist item has been added requiring the checklist to be referenced in the applicable phase summary report.

Attachment A – IEEE 1012-1998 Table 2 - Minimum V&V Tasks Assigned to Each Software Integrity Level a,c

Attachment A – IEEE 1012-1998 Table 2 - Minimum V&V Tasks Assigned to Each Software Integrity Level a,c

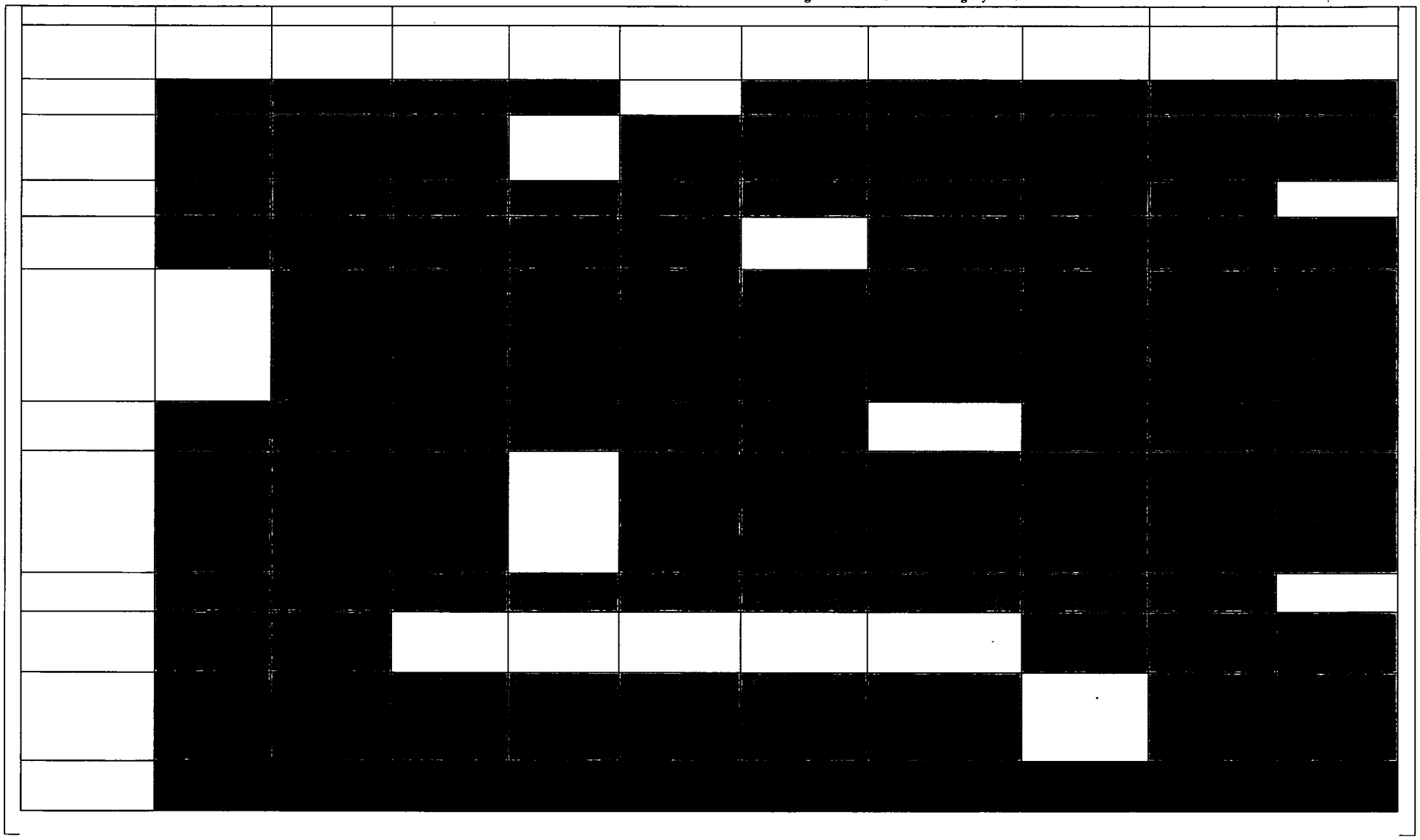
Attachment A – IEEE 1012-1998 Table 2 - Minimum V&V Tasks Assigned to Each Software Integrity Level

a,c

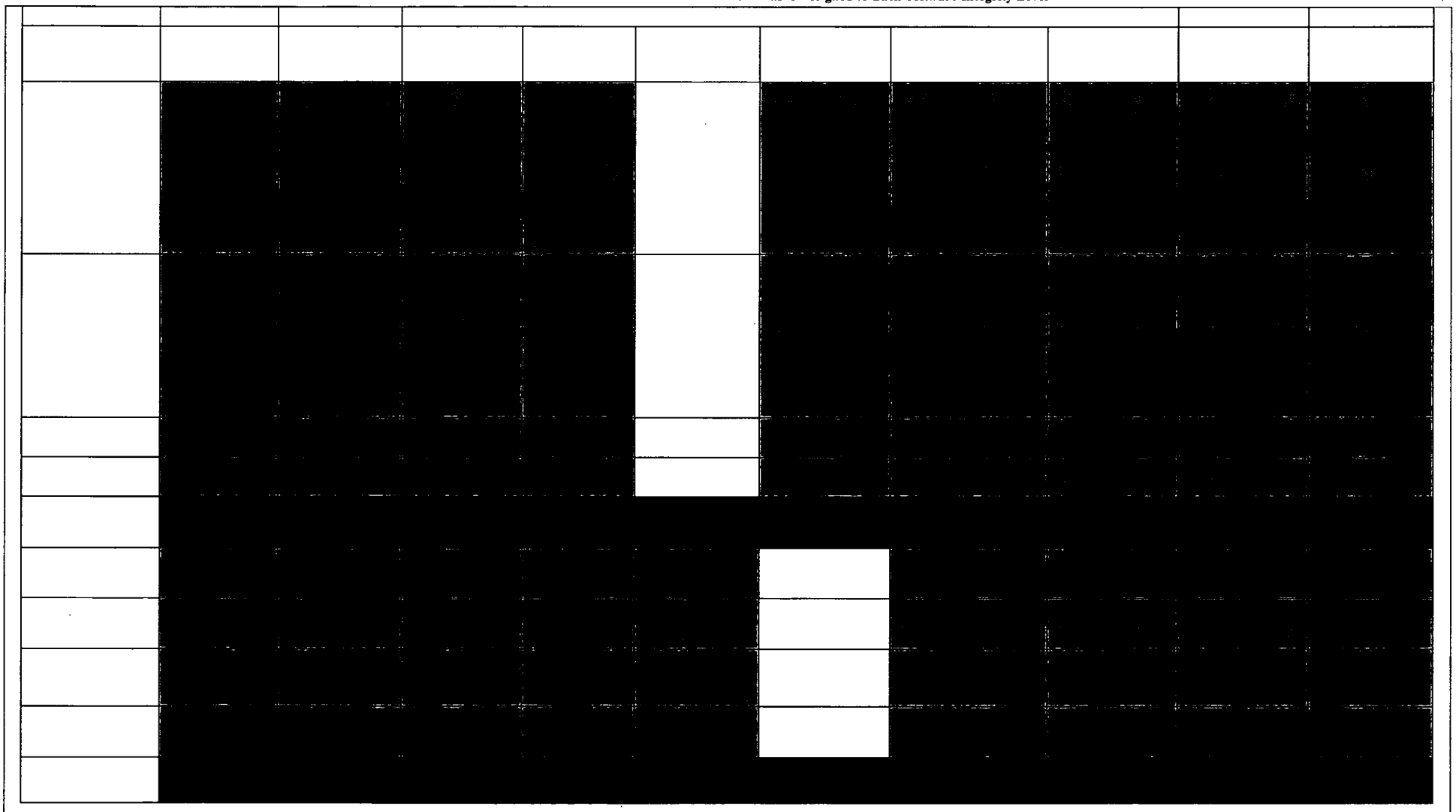


Attachment A – IEEE 1012-1998 Table 2 - Minimum V&V Tasks Assigned to Each Software Integrity Level

a.c



Attachment A – IEEE 1012-1998 Table 2 - Minimum V&V Tasks Assigned to Each Software Integrity Level a,c



Attachment A – IEEE 1012-1998 Table 2 - Minimum V&V Tasks Assigned to Each Software Integrity Level a,c

Attachment B – Software Program Manual for Common Q Systems (WCAP-16096) Compliance to RG 1.152, Rev. 3

a,c

Attachment C – Table II. Information Requirements

SPM Section Number	Description of Requirement	Output Document	Output Phase
1.4.2	Training Record For SPM	Training Record	N/A
3.1.2	Defining Acceptable Risks	Project Plan	Concept
3.3.2	A detailed schedule	Project Plan	Concept
3.3.2	Resource Plan	Project Plan	Concept
3.3.5.10	Software User Documentation	Technical Manual	Test Phase
3.3.5.11	Results of Software Safety Requirements Analysis	IV&V Report	Requirements Phase
3.3.5.12	Results of Software Safety Design Analysis	IV&V Report	Design Phase
3.3.5.13	Results of Software Safety Code Analysis	IV&V Report	Implementation Phase
3.3.5.14	Results of Software Safety Test Analysis	IV&V Report	Test Phase
3.3.5.15	Results of Software Safety Change Analysis	IV&V Report	Maintenance Phase
3.3.6	Software Hazards	Software Hazards Analysis Report	Requirements Phase
3.3.6	Results of IV&V Analyses	IV&V Report	All Phases
3.3.6	Information on suspected or confirmed safety problems	IV&V Report	Test Phase
3.3.6	Results of audits performed on software safety program tasks	Audit Report	Test Phase
3.3.6	Results of safety tests conducted on the system	Test Reports	Test Phase
3.3.6	Training Records	Training Record	N/A
3.3.6	Software Safety Certification – Code Certificate	IV&V Report	Test Phase
3.3.6	Tracking system to ensure hazards and their statuses are tracked throughout software life cycle	Requirements Traceability Matrix	All Phases
3.3.10	Project Manager approves the use of any tool – approval implicit by listing tool in Plan	Project Plan	Concept Phase
3.4.1	Software Hazards Analysis	Software Hazards Analysis Report	Requirements Phase
3.4.2	Software Safety Requirements Analysis	IV&V Report	Requirements Phase
3.4.3	Software Safety Design Analysis	IV&V Report	Design Phase
3.4.4	Software Safety Code Analysis	IV&V Report	Implementation Phase

Attachment C – Table II. Information Requirements

SPM Section Number	Description of Requirement	Output Document	Output Phase
3.4.5	Software Integration Safety Analysis	IV&V Report	Test Phase
3.4.6	Software Safety Test Analysis	IV&V Report	Test Phase
3.4.7	Software Installation Safety Analysis	IV&V Report	Installation and Checkout Phase
3.4.8	Software Safety Change Analysis	IV&V Report	Maintenance Phase
3.5	Training in SPM Section 10	Training Record	Installation and Checkout Phase
3.5.1	Review of Training Materials	IV&V Report	Installation and Checkout Phase
3.5.1	Personnel Training	Training Record	Installation and Checkout Phase
3.5.2.1	Review of Installation documentation	IV&V Report	N/A
3.5.2.2	Software Installation and Startup Procedure	Technical Manual	Installation and Checkout Phase
3.5.3	Procedures to verify software integrity to detect unauthorized modification of code or data	Technical Manual	Installation and Checkout Phase
4.1.1	Documenting Software Classification	Safety Classification Record	Concept Phase
4.1.2	Commercial Grade Dedication	Commercial Grade Dedication Report	N/A
4.3.2.1	Quality Assurance Planning	Project Quality Plan	Concept Phase
4.3.2.4	Verification of module code listings	Code Review Reports	Implementation Phase
4.3.2.6	Exception Report Log	Exception Report Database	Installation and Checkout Phase
4.3.2.6	Exception Report	Exception Report Database	Installation and Checkout Phase
4.5.1	Work Instructions	Any document required to supplement the SPM (such as Coding Standards and Guidelines Document)	N/A (Generic)
4.5.2.1	Coding Standards	Coding Standards and Guidelines Document	N/A (Generic)
4.5.2.4	Metric Reporting	Test Reports	Test Phase
4.6.2.1	Software Requirements Review	IV&V Report	Requirements Phase

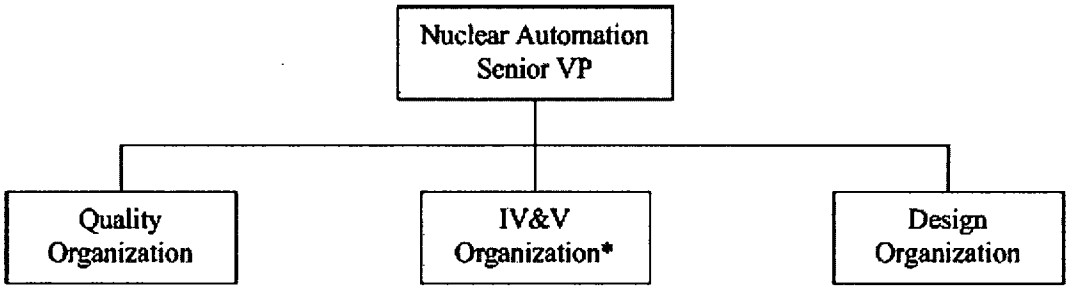
Attachment C – Table II. Information Requirements

SPM Section Number	Description of Requirement	Output Document	Output Phase
4.6.2.2.1	Architecture Design Review	IV&V Report	Design Phase
4.6.2.2.2	Critical Design Review	IV&V Report	Design Phase
4.6.2.3	Code Certification	Code Review Reports	Implementation Phase
4.6.2.4	SVVP Review	SPM	Concept Phase
4.6.2.5	Functional Review	IV&V Report	Test Phase
4.6.2.6	Physical Review	Certificate of Conformance and IV&V Report	Installation and Checkout Phase
4.6.2.7	In-process Audits	Audit Report	All Phases
4.6.2.8	Managerial Reviews	Audit Report	All Phases
4.6.2.9	Software Configuration Management Plan Review	IV&V Report	Concept Phase
4.6.2.10	Post Mortem Review	CAPs (LN Database)	Installation and Checkout Phase
5.1.4	Project-Specific IV&V Plan Activities	Project Plan	Concept Phase
5.4.5.2	IV&V Checklists	IV&V Report	All Phases
5.4.5.2	Review Changes to COTS software	Commercial Grade Dedication Report	Concept Phase
5.4.5.3	Requirements Traceability Analysis	RTM or Requirements Management Database	Requirements thru Test Phase
5.4.5.4	Database reviews (see also 5.5.5.2 #5)	Implementation Phase Checklist in IV&V Report	Implementation Phase
5.5.1	Baseline Change Assessment	Regression Analysis	All Phases
5.5.3.2	Software Safety Analyses	IV&V Report	Requirements Phase
5.5.4.2	Software Safety Design Analyses	IV&V Report	Design Phase
5.5.5.2	Software Safety Code Analyses	IV&V Report	Implementation Phase
5.5.6	Software Safety Test Analysis	Test Phase Checklist in IV&V Report	Test Phase
5.5.6.3	Code Certificate	IV&V Report	Test Phase
5.5.7.1	Installation Procedures, System Generation Procedures, User Documentation	Technical Manual	Installation and Checkout Phase

Attachment C – Table II. Information Requirements

SPM Section Number	Description of Requirement	Output Document	Output Phase
5.5.7.2	Training Material	Training Program Per Customer Requirements	Installation and Checkout Phase
5.5.8	Regression Analysis	IV&V Report or separately prepared document	Operations and Maintenance Phase
5.6.1	Discrepancy Reports	Exception Record Database; Status defined in IV&V Report	All Phases
6.2.2.1	Define ENM software items which are to be controlled via SCM	Project Quality Plan	Requirements Phase
6.2.2.3	Define software items which are to be controlled via SCM	Project Plan	Implementation Phase
6.3.2	Master list of software under configuration control for a project	Software Release Record	Implementation Phase
6.3.2	Software Change Request	Database	Implementation Phase, Test Phase, and Maintenance Phase
6.3.2	Software Change Request Log	Database	Implementation Phase, Test Phase, and Maintenance Phase
6.3.3	Configuration Status Accounting	Configuration Management Release Report	All Phases
8.3.2.1	Feasibility Analysis	Project Quality Plan	Concept Phase
8.3.2.2	Detailed Analysis	SysRS, SRS, Test Plan, PQP	Requirements Phase
8.5.2.4	Risk Analysis	Project Quality Plan	Implementation Phase
10.2	Justification for not performing complete system retesting	Regression Analysis in Exception Report or SCR	Test Phase
10.2	Exception Reports	Database	All Phases

Attachment D – Exhibit 2-1 Design/IV&V Team Organization



* The IV&V Organization is comprised of multiple IV&V groups.

Attachment E1 – AC160 Application Code Review Checklist

a,c

[ ]

Attachment E2 – Software Module Review Checklist

a,c

[

]

Attachment E3 – FPD Software Module Review Checklist

a,c

[ ]